(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2004-535623
(P2004-535623A)
(43)公表日　平成16年11月25日(2004.11.25)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	560B	5B017
	G06F 12/14	520D	
	G06F 12/14	530C	
	G06F 12/14	530E	

審査請求 未請求　予備審査請求 有　（全 70 頁）

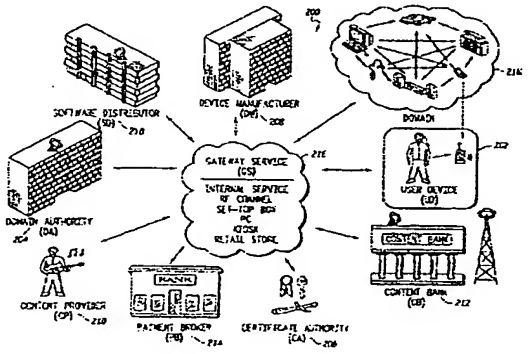
(21)出願番号	特願2002-584178 (P2002-584178)
(86)(22)出願日	平成14年3月12日 (2002.3.12)
(85)翻訳文提出日	平成15年10月20日 (2003.10.20)
(86)国際出願番号	PCT/US2002/007398
(87)国際公開番号	WO2002/086725
(87)国際公開日	平成14年10月31日 (2002.10.31)
(31)優先権主張番号	60/284,739
(32)優先日	平成13年4月18日 (2001.4.18)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	09/942,010
(32)優先日	平成13年8月29日 (2001.8.29)
(33)優先権主張国	米国 (US)

(71)出願人　390009597
モトローラ・インコーポレイテッド
MOTOROLA INCORPORATED
アメリカ合衆国イリノイ州シャンバーグ、イースト・アルゴンクイン・ロード１３０３
(74)代理人　100116322
弁理士　桑垣　衛
(72)発明者　メッサージス、トーマス　エス.
アメリカ合衆国　６０１９３　イリノイ州　シャンバーグ　ブルックストン　ドライブ　１５１

最終頁に続く

(54)【発明の名称】デジタル電子通信コンテンツを安全かつ便利に管理するためのシステムおよび方法

(57)【要約】
ドメインベースのデジタル著作権管理のための方法および装置（２００）を用いる。



【特許請求の範囲】
【請求項１】
ドメインベースのデジタル著作権管理環境において動作可能な通信機器であり、
処理部と、
前記処理部に接続されて該処理部によって制御され、前記通信機器に送信されるメッセージを受信可能な受信部と、
前記処理部に接続されて該処理部によって制御され、前記通信機器の出力メッセージを送信可能な送信部と、
前記処理部に接続され、前記ドメインベースのデジタル著作権管理環境における前記通信機器の動作を制御するデジタル著作権管理モジュールとを備え、
前記通信機器の前記デジタル著作権管理モジュールは、前記ドメインベースのデジタル著作権管理環境のドメイン管理機関と協働して暗号鍵を共有する１つ以上の通信機器を有するドメインに前記通信機器を選択的に加入させ、これにより前記通信機器に前記ドメインのメンバーシップに基づいてデジタルコンテンツの選択的受信および暗号解読を許可するように動作可能な通信機器。
【請求項２】
前記送信部は、通信範囲の限定された通信装置であって、前記デジタルコンテンツを前記限定された通信範囲内の信頼された通信装置に送信するように動作可能な請求項１記載の通信機器。
【請求項３】
前記デジタル著作権管理モジュールは、ユーザの要求を受けて前記通信機器の前記送信部に前記通信機器の前記ドメインへの登録の要求をドメイン管理機関へ送信させ、
前記通信機器が１つ以上の有効な暗号要素へのアクセス権があると判断されたことを受けて、前記デジタル著作権管理モジュールは、前記通信機器を前記ドメインに結合するために、前記通信機器の前記受信部に前記ドメインの前記暗号鍵を通信チャンネルを介して前記ドメイン管理機関から受信させる請求項１記載の通信機器。
【請求項４】
前記デジタル著作権管理モジュールは、前記ドメイン管理機関と協働して前記通信機器を前記ドメインから脱退させ、
前記ドメインの前記ユーザによる前記通信機器の脱退の要求があった場合、前記デジタル著作権管理モジュールは、前記通信機器の前記送信部に前記通信機器の前記ドメインからの脱退の要求を送信させ、
前記脱退の要求を受けて、前記通信機器は前記ドメインの前記暗号鍵を前記通信機器から消去するよう指示する命令を前記ドメイン管理機関から前記安全な通信チャンネルを介して受信し、
前記命令を前記ドメイン管理機関から受信すると、前記デジタル著作権管理モジュールは前記ドメインの前記暗号鍵を消去する請求項３記載の通信機器。
【請求項５】
前記通信機器の前記デジタル著作権管理モジュールが前記送信部にデジタルコンテンツを求める要求を送信させたことを受けて、前記通信機器の前記デジタル著作権管理モジュールと前記ドメイン管理機関の少なくとも一方が前記ドメインの信頼性を確認し、
前記ドメインの信頼性が確認されると、前記通信機器が登録されている前記ドメインの前記暗号鍵に結合された前記要求されたデジタルコンテンツの暗号化された形式を前記通信機器の前記受信部が受信する請求項１記載の通信機器。
【請求項６】
前記通信機器の前記デジタル著作権管理モジュールは、前記要求されたデジタルコンテンツに関連付けられ、前記要求されたデジタルコンテンツを含むコンテンツパッケージ内に含まれて前記受信部によって受信される使用規則を実施する請求項１記載の通信機器。
【請求項７】
前記コンテンツパッケージは、前記使用規則を含む二進表現の権利テーブルを有する請求

項６記載の通信機器。
【請求項８】
前記二進表現の権利テーブルは、あらかじめ定義されたトークンを有した複数の部分を備える請求項７記載の通信機器。
【請求項９】
前記通信機器の前記送信部が前記ドメインの第二の通信機器から前記デジタルコンテンツを求める要求を受けたことを受けて、前記デジタル著作権管理モジュールは、前記送信部に前記要求されたデジタルコンテンツを格納部から前記第二の通信機器へ送信させる請求項１記載の通信機器。
【請求項１０】
前記通信機器の前記ユーザの要求を受けて、前記デジタル著作権管理モジュールは、前記送信部に、前記ドメインにおいて入手不可能なデジタルコンテンツを求める要求を送信させ、
前記ドメインの信頼性が確認された後、前記通信機器が登録されている前記ドメインの前記暗号鍵に結合された前記要求されたデジタルコンテンツの暗号化された形式を前記受信部が受信する請求項１記載の通信機器。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般には通信システムに関し、より詳細には、安全確実なデジタルコンテンツへのアクセスを実現するためのコンテンツ管理システムに関する。
【背景技術】
【０００２】
デジタルコンテンツの市場は今後膨大な成長を続けることが見込まれている。例えば、インターネットは事業や商売の行われ方に様々な変化をもたらしてきており、消費者は自宅のパソコンから容易に様々な製品を見て購入することが可能となっている。そのようにして購入された製品は、ＵＰＳ（Ｕｎｉｔｅｄ　Ｐａｒｃｅｌ　Ｓｅｒｖｉｃｅ）宅配便やＦｅｄＥｘ等の在来の手段によって自宅に配送可能である。一方、製品が物としての製品ではなくデジタル製品の場合には、インターネットそのものを製品の配送に用いることができる。実際には驚くべき数の製品がデジタル的に表現可能であり、インターネットを用いて購入者に転送可能である。そのような売買の可能性のあるデジタル物品としては、音楽、ソフトウェア、ビデオ、本などがよく言及されるが、例えばチケット、絵画や写真、スタンプ等もデジタル物品としての可能性がある。以上に挙げたものはすべて「コンテンツ」の例である。ここで「コンテンツ」とは、鍵ソフトにより鍵を掛けてリアルタイムで配送可能なデジタル情報（例えばストリーミングデータ）や、いずれかの場所に格納されて後からアクセスされるデータを指す。このようなコンテンツとしては、オーディオブック、ビデオ映像、コンピュータゲーム、ビデオクリップ、ＤＶＤ／ＭＰＥＧムービー、ＭＰ３音楽ファイル、ビジネスデータ（電子メール、文書等）、携帯機器のアップグレード（携帯電話機の三者通話、種々の着信音モード等）などがあり得る。
【０００３】
インターネットや性能向上した携帯コンピュータ機器の出現に伴い、消費者は間もなくデジタル情報への時間と場所を問わない継続的なアクセスを望むようになることが見込まれ、機器間（ポケベル、携帯電話、セットトップボックス、家庭用コンピュータ、自動車用娯楽システム、等）の相互接続の実現による様々な新規ビジネスの可能性が開けている。ＭＰ３音楽ファイル、コンピュータゲーム、ＤＶＤムービー等のデジタルコンテンツの人気は急上昇しており、種々の無線機器はこのようなデジタルコンテンツへのアクセスを直感的で容易なものにしつつある。
【０００４】
一方、デジタルコンテンツが持つ価値、急上昇する人気およびその利用のしやすさから、コンテンツの所有者側には、上記のような新型機器の登場により自分のデジタルコンテン

ツが不法コピーや不法配布の被害を受けやすくなるのではないかとの懸念が持ち上がっている。現在例えばナップスター（Ｎａｐｓｔａｒ）等を用いてインターネットで流行している海賊行為の拡大を防止するために、コンテンツ提供者らは安全なコンテンツ管理機構に頼ることを考慮中である。コンテンツの提供者らは、自身の権利が安全に保護され、正当な配布ルールが確実に守られることを希望している。情報に基盤を置いた経済機構においてデジタルデータはそれ固有の価値を有しており、そのために所有権や著作権法が遵守される必要がある。

【０００５】

このようなデジタルコンテンツ市場の実現を目指し、また一方でコンテンツ提供者側の満足を得るために、多くのハードウェア及びソフトウェア業者がデジタルコンテンツを安全に取り扱うための枠組みの導入を開始している。「デジタル著作権管理（ＤＲＭ：Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ）」とは、権利の保護とデジタル情報のアクセス及び処理に関するルールの管理を示すためによく引用される用語である。これらの権利やルールは、誰が物品を所有するのか、いつどのようにして物品にアクセス可能か、物品の購入にいくらかかるのかなど、デジタル物品の様々な側面を決定付ける。あるデジタル物品に関係した諸規則が極めて複雑なものになることはよくあり、そのため、ソフトウェアシステムには、これらの規則を構築し、指定し、管理することがしばしば必要とされる。

【０００６】

しかし、新しく登場してきた枠組みの多くは、消費者が利用するには煩雑過ぎて不便とされ評判が悪い。デジタルコンテンツ保護のための安全な方法は、エンドユーザの使い勝手を犠牲にして成り立つことが多く、より良い新しい解決方法が求められていることは明らかである。

【０００７】

現在広く検討されているデジタル著作権管理の構想として、コピーベースの手法がある。この種のシステムでは、コンテンツのマスターコピーが、パソコンやサーバ上で動くデジタル著作権管理システムにより格納され管理される。従来のチェックイン／チェックアウト方式の手法では、要求されたデジタルコンテンツ情報の提供の可否やいつ提供すべきかの決定を任された「信頼されたシステム」に対してコンテンツが暗号を用いて結合されており、通常は、一つのデジタルコンテンツに対して有限数のコピーが可能に設定されている。このコピーベースの手法では、デジタルマスターのコピーの送出に対して責任を負う「デジタル著作権管理カーネル」が用いられる。ユーザは自分のユーザ機器のためのコピーを要求し、デジタル著作権管理カーネルは送出されたコピーの数を監視する。通信機器（例えば携帯無線機器）が一つのデジタルコンテンツのコピーをチェックアウトする（引き出す）場合、前記信頼されたシステムは、そのコンテンツのコピーをコンテンツ受信側の機器と暗号を用いて結合し、チェックアウト可能コピー数を一つ減らす。一方、コピーが返却された場合には、前記信頼されたシステムはチェックアウト可能コピー数を一つ増やす。可能コピー数が０の場合、前記信頼されたシステムは、コンテンツのコピーのチェックアウトを許可しない。

【０００８】

以下に一例として、デジタル音楽コンテンツの制御のために楽曲のチェックイン／チェックアウト方針を管理する枠組みとしてのＳＤＭＩ（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ　Ｍｕｓｉｃ　Ｉｎｉｔｉａｔｉｖｅ）フレームワークについて考察する。楽曲のマスターコピーは、パソコンやサーバ上で動くデジタル著作権管理システムにより格納され管理され、１曲に対してチェックアウト可能なコピーの数は固定される。従って、すべてのコピーがチェックアウトされていれば、一つのコピーがチェックイン（返却）されるまでは新しいコピーを送出することができない。楽曲の安全を確保するため、前記ＳＤＭＩフレームワークには、このチェックアウトがコンテンツを携帯機器に転送するための唯一の手段であると規定してあり、これはユーザにとっては極めて使い勝手が悪く不親切なものである。従って、このＳＤＭＩシステムは公衆から非常に低い評価を受けたデジタル著作権管理機

構の一つとなっている。

【０００９】

典型的な筋書きとしては、ユーザは自分の音楽コレクションを自分のパソコン内の暗号で保護された音楽ライブラリに保存し、携帯音楽プレーヤーを所有するユーザは自分の音楽ライブラリから音楽をそのプレーヤーにコピーすることができる。デジタル著作権管理システムはライブラリを制御し、ライブラリを出ることを許可されるコピーの数に責任を持つ。ＳＤＭＩに準拠したシステムにおいては、デジタル著作権管理ソフトウェアが楽曲のチェックイン／チェックアウト方針を管理する。ＳＤＭＩのためには、１曲に対するチェックアウト可能なコピーの数が固定され、すべてのコピーがチェックアウトされている場合、少なくとも１つのコピーがチェックイン（返却）されるまでは他の機器によるチェックアウトはできない。楽曲を安全に保つためには、このチェックイン／チェックアウトが、楽曲を携帯機器に転送するための唯一の手段となる。

【００１０】

図１に、コンテンツに対する海賊行為を防止するためのコピーベースのシステム１００の一例を示す。この例では、コンテンツは購入側ホストに結合されることにより暗号によって保護される。本システムにおいて、コンテンツプロバイダ１０２はコンテンツライブラリ１０４を維持する。一つのコンテンツが購入された場合、コンテンツプロバイダ１０２は当該コンテンツを購入側ホストのパソコンまたはサーバ１１０に暗号を用いて結合する。ホスト１１０はデジタル著作権管理システム１１４を有しており、コンテンツをプロバイダから受信してこれを暗号化コンテンツライブラリ１１２に格納する。ホストのデジタル著作権管理システム１１４は、各コンテンツに対する可能コピー数の監視に用いられるコンテンツリスト１１６を保持する。携帯機器１１８ａ，１１８ｂ，１１８ｃは、いずれもコンテンツを要求することができる。利用可能なコピーがあれば、デジタル著作権管理システム１１４は暗号化処理を用いて携帯機器にコピーを転送する。デジタル著作権管理システム１１４はさらに転送されたコンテンツに対して可能コピー数を一つ減らす。図１の例では、各コンテンツに対して３つのコピーがあるが、例えば番号＃４５３６の付けられたコンテンツはどの機器からもチェックアウトを受けておらず、まだ３個のコピーが残っている。一方、番号＃６１２３のコンテンツは現在携帯機器１１８ａ，１１８ｂ，１１８ｃによるチェックアウトを受けており、チェックアウト可能コピー数は０である。デジタル著作権管理システム１１４は、携帯機器１１８ａ，１１８ｂ，１１８ｃのいずれかがこのコピーをチェックインするまでは、第４の機器に番号＃６１２３のコンテンツのチェックアウトを許可しない。

【００１１】

総体的に見ると、デジタル音楽へのアクセス制御のためのこの従来の方法は多くの人から押しつけがましく面倒なものとして捉えられている。特に厄介なのが、ユーザが新しい曲をロードする前に自分の持つコピーをチェックインしなければならない事である。このシステムのユーザは、自分の機器に曲を転送する毎にセキュリティーコントロールに直面することになる。コピーコントロールセキュリティーを実施しない他の類似したシステムではこのようなチェックインの要求はなく、このためユーザの音楽体験は大きく広がることになる。しかしもちろん、セキュリティーがなければデジタルコンテンツに対する海賊行為が極めて起こりやすくなり、コンテンツ提供者らはそのようなシステムにコンテンツを供給したがらなくなるであろう。

【００１２】

セキュリティーの実施はバランスよく行われる必要がある。セキュリティーの低すぎるシステムはコンテンツ提供者に信頼されないが、セキュリティーが厳重過ぎるシステムは顧客に好まれない。ＳＤＭＩのために提案された従来のコピーベースのチェックイン／チェックアウトによる各方法やその他のデジタル著作権管理システムはセキュリティーを提供するが、エンドユーザのニーズを満足させるものではない。システムは、コンテンツがユーザ機器に移動される毎にユーザがセキュリティーに遭遇することを要求し、このような過剰なセキュリティーのためにユーザの体験は貧しいものになってしまう。コンテンツが

頻繁にアクセスされる信頼されたシステムにおいて、コンテンツを要求するユーザ機器にコンテンツが移動される場合やチェックインのためユーザ機器からコンテンツが移動される場合の上記手法は、リモートサーバ上でよりもユーザのローカルサーバまたはパソコン上で実施されることが多く、開放されたシステムの中でパソコンや他のローカルサーバ機器によってセキュリティーを維持し確保することは困難である。

【００１３】

上記内容から、デジタルコンテンツの安全で欠陥のない管理のための方法として、取り扱い易く、かつ適切なセキュリティーを維持することのできるものがこの技術分野においてまだ達成されていないことがわかる。デジタルコンテンツのセキュリティーの要求は、その一方でエンドユーザに対する楽しいユーザ体験の提供を確保しながら守られるべきである。

【発明を実施するための最良の形態】

【００１４】

本発明の新規な特色については特許請求の範囲に示されているが、実施の形態の詳細な記載を添付図面と共に参照することにより、本発明の内容に加えてその好適な使用形態、更にその目的や長所を最も良く理解することが可能である。

【００１５】

本発明には様々な形の実施の形態が可能であるが、以下に具体的な実施の形態を図面を参照して詳細に説明する。この開示は本発明の諸原理を示すための一例とみなされるべきものであり、記載された特定の実施の形態により本発明が限定されるべきではないことが理解されるはずである。以下の記述において、類似した参照番号は、いくつかの図面における同一、類似または対応する部品を示すために用いられる。

【００１６】

本発明は、従来の煩雑なコピーベースのデジタル著作権管理システムとは対照的に、消費者が望みのデジタルコンテンツにアクセスするための使いやすい方法として、ドメインベースのデジタル著作権管理システムを用いてコンテンツを管理し海賊行為を防止する方法を提供する。本発明では、コンテンツがユーザ機器（ＵＤ：Ｕｓｅｒ　Ｄｅｖｉｃｅ）等の通信機器を出入りする度にユーザがセキュリティーによる制約に遭遇するチェックイン／チェックアウト方針に基づくコンテンツへのアクセス制限ではなく、ドメインベースの手法を用いてデジタルコンテンツへのアクセスを管理する。このドメインベースの手法では、ユーザがセキュリティーと格闘する必要があるのは新しいユーザ機器を購入する時つまりドメインに追加する時、または古いユーザ機器をドメインから取り除く時のみとなる。コンテンツへのアクセス権は、典型的にはあるドメインの限られた数の登録された機器のみに制限される。ここで、ドメインとは、そのドメインに関連付けられた共通の暗号鍵（ｃｒｙｐｔｏｇｒａｐｈｉｃ　ｋｅｙ）を共有する１つ以上のユーザ機器（通常は所定数以下の通信機器）を含むものである。複数の機器を所有するユーザは、それらを同一のドメインに登録したいと考えるであろう。図２を参照すると、本発明による典型的なデジタル著作権管理システム２００に関与する可能性のある構成要素の例が示されている。なお、ここに描かれた種々の構成要素により示される機能性を他の要素を用いて実現することや、種々の構成要素による機能性をより少数または多数の要素によって実現することが本発明の精神と範囲から逸脱することなく可能であることは充分認識されるはずである。消費者またはユーザは、通信機器２０２（以下、ユーザ機器という）を購入することができる。このユーザ機器は、デジタルコンテンツにアクセスし、かつ／または操作するための電子機器であればどのようなものでもよい。ユーザ機器の例としては、音楽を再生（表現）可能な携帯電話機、カーステレオ、セットトップボックス、パソコン等がある。一人のユーザは、自身が所属する１つ以上のドメインに登録したい複数のユーザ機器を所有している場合があり（ドメインの重複があってもなくてもよい）、また現在所有していなくても所有するようになる可能性が高い。第１のドメインの少なくとも１つの通信用ユーザ機器が同時に第２のドメインにも登録されている場合、この第１および第２ドメインは、当該機器に関する重複したドメインと呼ばれる。図３に、重複したドメインの一例（子供

２１６、親２１６、ビジネス２１６）を示す。ユーザ機器は、携帯電話機等のように携帯無線式であってよく、従って無線インターネットに接続することは容易である。ブルートゥース規格で実現されているような赤外線（ＩＲ）や周波数限定の技術を用いてもよい。ブルートゥース規格のユーザ機器は、パソコンやキオスク端末等のブリッジ機器を用いてインターネットに接続してもよい。

【００１７】

ドメイン管理機関（ＤＡ：Ｄｏｍａｉｎ　Ａｕｔｈｏｒｉｔｙ）２０４は、ユーザ機器のドメインへの登録（追加）や登録解除（除去）を担当する。ドメイン管理機関が機器をドメインに追加する場合は、まずその機器が正規の機器かどうかを確認した上で追加する。正規の機器かどうかは、正規の機器のみが適切な証明書や鍵を利用できることから判別できる。ドメイン管理機関は更に、機器の鍵や証明書がまだ有効であるかを確認するために証明書管理機関（ＣＡ：Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）２０６が提供する取消リストを参照することができる。機器が本物と判断されれば、ドメイン管理機関はユーザ機器に、適切な鍵や証明書や機器をドメインに登録するために必要なコマンドを送信する。ドメイン管理機関は更に、ドメインデータを消去するコマンドを機器に送信して該機器をドメインから除去することもできる。更に、ドメイン管理機関はドメイン内に許可されるユーザ機器の数の制限や、機器の不正な登録や登録解除の監視を担当する。

【００１８】

機器製造業者（ＤＭ：Ｄｅｖｉｃｅ　Ｍａｎｕｆａｃｔｕｒｅｒ）２０８は、コンテンツの使用規則を実行する機能または安全なデジタル著作権管理機能を備えたユーザ機器を製造する。例えば、機器製造業者は、各ユーザ機器がデジタル著作権管理システムの他の構成要素から一意に識別可能となるように、ユーザ機器に安全な形で鍵を組み込むこともできる。機器製造業者はまた、証明書管理機関の認証鍵（ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｋｅｙ）、証明書または他の秘密情報の機器への組み込みも担当する。ユーザ機器がドメインベースのデジタル著作権管理システム内で動作するために使用されるソフトウェアは、ユーザ機器に予めインストールされていても、後にソフトウェア配給元（ＳＤ：Ｓｏｆｔｗａｒｅ　Ｄｉｓｔｒｉｂｕｔｏｒ）２１８から入手される形でもよい。

【００１９】

コンテンツプロバイダ（ＣＰ：Ｃｏｎｔｅｎｔｓ　Ｐｒｏｖｉｄｅｒ）２１０は、コンテンツをドメインの登録された各ユーザ機器に対して販売または供給する。コンテンツプロバイダは、例えば、そのコンテンツを製作したアーティスト、大型のコンテンツ供給元、コンテンツを販売するオンラインストア等でありうる。コンテンツプロバイダの重要な仕事は、一揃いの規則を作り上げ、その規則をコンテンツとこれを購入するドメインとに関連付けることである。例えば、コンテンツプロバイダであるバンドＸＹＺが「ＡＢＣ」という最新のシングルに対してどのような規則を設けられるかを考えてみよう。シングル「ＡＢＣ」を通常通りレコーディングした後、ファイル「ＡＢＣ．ｗａｖ」を作成した彼らは、この曲のインターネットによる販売にも関心があるため、曲をＭＰ３ファイルに圧縮してファイル「ＡＢＣ．ｍｐ３」を作成する。このＭＰ３ファイルは次に暗号化され、使用規則（この曲の再生が誰に許されるか、コピーが誰に許されるか、編集が誰に許されるか、曲の貸し出しが許されるか、曲の再生に関する料金体系、曲に対して規則を付加できるかおよび誰が付加できるか等）がこれに関連付けられる。このような使用規則は、標準的なアプリケーションソフトウェアによって添付することができる。コンテンツプロバイダがコンテンツをパッケージ化する段階では、コンテンツそのものより、いかにコンテンツ規則を操作するかが重要となる。

【００２０】

コンテンツの格納は様々な形で行われ、その方法は主にコンテンツの種類や、ユーザ機器、ドメイン及び全システムのそれぞれの格納力によって決定される。コンテンツは、ユーザ機器に格納されたり、例えばコンテンツバンク（ＣＢ：Ｃｏｎｔｅｎｔｓ　Ｂａｎｋ）２１２のオンラインアカウントに送られたり、ユーザのパソコンや他の利用可能なサーバにコピーされたり、消費者にレガシーコンテンツとして配布されたりする。このコンテン

ツバンクは、ユーザのコンテンツアカウントを格納し維持する責任を負う事業体である。アカウントにおけるコンテンツは、必ずしも単独のエンドユーザに関連付けられたアカウント内に格納される必要はなく、その代わりに、そのコンテンツの一つのコピーへのポインタが保持されるような形も可能である。それによりユーザのコンテンツアカウントのサイズの肥大化を確実に防止できる。例えば、エンドユーザがある曲を購入した場合、その曲はそのエンドユーザのコンテンツアカウントに転送され、そのユーザの携帯ユーザ機器に格納される。この場合、そのコンテンツに関連付けられた規則を、そのコンテンツアカウントや携帯機器に転送してもよい。ユーザがコンテンツをそのユーザ機器にロードしようと決めた場合、コンテンツバンクは、該コンテンツを真正の、規則を守る機器（この場合は当該ユーザ機器）にのみ供給することを保証する責任を持ち、そのために、証明書管理機関２０６が当該ユーザ機器を証明するために発行した証明書や秘密情報を用いることができる。

【００２１】

当該デジタル著作権管理システムにおいて要求されるセキュリティーの維持のために用いられる公開鍵は、証明書管理機関２０６によって管理され、そのサービス及び／又はコンテンツに対する支払いは、支払いブローカー（ＰＢ：Ｐａｙｍｅｎｔ　Ｂｒｏｋｅｒ）２１４によって管理される。証明書管理機関とは、デジタル証明書、公開鍵／秘密鍵の対、またはコンテンツが有効かつ安全な機器によって取り扱われているかの確認に用いられるその他の物を管理する例えば信頼された第三者機関または会社である。この確認を遂行するための方法としては、公開鍵、デジタル署名の機構、または秘密共有の機構がありうる。公開鍵に基づく機構では、デジタル著作権管理システムにおける構成要素および機器が本当にそれらが主張するものであることを証明するために証明書を用いることができる。秘密共有の機構においては、証明書管理機関は共有された秘密の配布に対して責任を持つ。どちらの機構においても証明書管理機関は、機器製造業者、コンテンツ流通業者および支払いブローカーと合意・取り決めを行う必要がある。更に、証明書管理機関は証明書または秘密情報の発行および取消しのための方法を保有する必要がある。証明書管理機関はオフラインのシステムであることが望ましく、従って、コンテンツが表現される毎に証明書管理機関と接触する必要はない。

【００２２】

ゲートウェイサーバ（ＧＳ：Ｇａｔｅｗａｙ　Ｓｅｒｖｅｒ）２１６は、システムの構成要素間に通信チャンネルまたはリンクを提供し、各構成要素はかわるがわる直接に通信することができる。ゲートウェイサーバの例としては、インターネットや無線周波数で接続されたキオスク端末、セットトップボックス、パソコンがあるが、これに限定されるものではない。以下において、上記のデジタル著作権管理システムの各構成要素、特にユーザ機器やドメイン管理機関について更に詳細に述べる。

【００２３】

ユーザ機器２０２は、ドメイン管理機関２０４に登録することによって、特定のドメインに割り当てることができる。機器は、あるドメイン２１６に登録されれば、そのドメインに「加入」したことになる。同様に、機器はその登録を取り消すことによりドメインを「脱退」することができる。ドメイン管理機関２０４は、ドメイン２１６における機器の数の制限、機器がドメインに加入したり脱退したりできる回数の制限などの登録方針を実施する。ドメイン管理機関２０４はまた、どの機器がドメインに加入／脱退するかを追跡することにより、将来起こりうる不正行為を監視する。過剰な活動を行っている機器はシステムを悪用しようとしている可能性があり、そのような機器に対して以後の登録活動を禁止することもできる。

【００２４】

ドメイン管理機関２０４は、ドメインＩＤを付与することによって携帯機器をドメインに割り当てる。ドメインＩＤは、不正改竄防止の方法を用いて該機器に関連付けられている。このドメインＩＤのユーザ機器への関連付けは、組み込まれたシリアル番号と、秘密鍵や公開鍵証明書等の暗号部品とを用いて行うことができる。これらの暗号部品は、ユーザ

機器およびドメイン管理機関上で動作する安全なデジタル著作権管理システムによって操作される。ドメインへのアクセスを許可することができるのはドメイン管理機関のみであり、従ってドメイン管理機関は、システムからの搾取を狙っていない機器のみをドメインのメンバーとすることをコンテンツプロバイダらに対して保証する。

【００２５】

デジタルコンテンツを販売する場合、コンテンツプロバイダは、ユーザ機器および／またはドメイン管理機関に対して、特定のドメインについて証明するよう問い合わせることができる。この問い合わせ処理は、盗聴者やハッカーによるシステムからの搾取を確実に防止できるように標準的な暗号認証プロトコルを用いて行われる。ドメインが正当なものであると納得したコンテンツプロバイダは、暗号を用いてコンテンツを購入側ドメインのＩＤと結合することにより、当該コンテンツを販売することができる。このドメインの外の機器は、他のドメインに暗号を用いて結合されたコンテンツに対してはアクセスできないため、このコンテンツは海賊行為に対して安全である。

【００２６】

この暗号化されたコンテンツはこのシステムのどのホストＰＣ（パソコン）やサーバ上にも開放状態で保管することができ、どの携帯機器もこのコンテンツを要求することができる。ホストは、チェックアウト操作を行うのではなく、このコンテンツを単に要求元機器に転送する。このコンテンツは暗号を用いて特定のドメインと結合されているため、コンテンツのセキュリティーが保証される。ドメイン管理機関が各ドメインに対して限られた数の機器しか許可しないため、海賊行為や不正コピーされた音楽の蔓延を防止することができる。また、ユーザ機器内のデジタル著作権管理システムが不正改竄を防止するため、ハッカーによるコンテンツへの不正アクセスが不可能となる。

【００２７】

本発明のシステムにおけるセキュリティーは、ユーザによる機器のドメインへの加入／脱退登録の回数が少ないため、従来の場合と比較してより取り扱い易いものとなっている。従来のチェックイン／チェックアウトシステムでは、ユーザはコンテンツを自分の携帯機器にまたは携帯機器から転送する毎にセキュリティーによる制約に遭遇していたが、本発明では、ユーザがセキュリティーと格闘する必要があるのは新しい機器を購入する時またはユーザ機器を１つ以上のドメインに追加したい時に限られる。

【００２８】

図４は、デジタルコンテンツへのアクセスを安全に管理するためのドメインベースのデジタル著作権管理システムを更に説明するためのブロック図である。ドメイン管理機関は、例えば携帯ユーザ機器２０２$_1$，２０２$_2$，２０２$_4$等の通信機器をドメイン（本例ではドメインＸＢＤＡ４１０とドメインＺＸＺＰ４１２の２個を示す）に割り当て、所定のドメイン登録方針を実施する。コンテンツライブラリ４０４からのコンテンツは、パソコンまたはサーバ４０６にではなく、１つ以上のドメイン（４１０，４１２）に暗号を用いて結合されることにより、保護される。ドメインに結合された、つまりドメインによりコンテンツの受信が認可された機器のみが、この暗号を用いてドメインに結合されたコンテンツを受信することができる。図５に、家庭用コンピュータ、ＭＰ３プレーヤー、自動車用娯楽システム、セットトップボックス、携帯電話機、家庭用娯楽システム等の種々の機器を含んだドメイン５００の例を示すが、このように、ドメイン２１６に登録されたすべての機器は、該ドメイン内のコンテンツにアクセスできるという意味で、相互接続可能である。これはまた、一つのドメイン（例えばドメインＺＸＺＰ４１２）の機器は他のドメイン（例えばドメインＸＢＤＡ４１０）に暗号を用いて結合されたコンテンツにはアクセスできないことを意味する。図６に示すシステム６００の例では、ドメイン２１６はコンテンツバンク２１２と通信している２台の携帯電話機＃１，＃２と１台のＭＰ３プレーヤーを含んでいる。一方、該ドメイン外のヘッドホンとステレオはコンテンツバンク２１２のコンテンツアカウントにアクセスすることができない。なお、図４に示した暗号化されたコンテンツはパソコンまたはサーバ４０６の暗号化コンテンツライブラリ４０８に格納されているが、要望に応じて、この暗号化されたコンテンツを更に通信装置（例えば、２０

２$_1$，２０２$_2$，２０２$_4$で示した携帯機器１，２，３のいずれか）に格納してもよい。

【００２９】

本発明によるドメインベースのデジタル著作権管理システムおよび方法の構成要素間の通信チャンネルには当然、充分な強度の暗号化プロトコルが用いられるべきである。インターネット利用可能な機器との通信には、ＷＴＬＳクラス３やＴＬＳ等の標準的プロトコルを用いることができる。また、コンテンツ保護のためにはトリプルＤＥＳやＡＥＳ等の強力な共通鍵暗号法（ｓｙｍｍｅｔｒｉｃ－ｋｅｙ　ｃｒｙｐｔｏｇｒａｐｈｙ）を、認証および署名には楕円曲線またはＲＳＡ公開鍵暗号法を用いることができる。コンテンツの完全性はＳＨＡ－１等の安全なハッシュ関数を用いて維持可能である。ここで、ユーザ機器が機器製造業者によって製造される場合を一例として考察してみる。製造完了したユーザ機器には、（製造業者または他の信頼された管理機関により）正規品である証明が付けられる。この証明は、公開鍵または共有された秘密鍵によって確認可能な証明書を用いて実施することができる。証明されたユーザ機器はこの証明書（または証明書の参照先情報）およびこの証明書に対応する秘密鍵（ｓｅｃｒｅｔ　ｋｅｙ）を保持することになる。この秘密鍵は、証明書の公開鍵と対になる秘密鍵（ｐｒｉｖａｔｅ　ｋｅｙ）でも、デジタル著作権管理システムの前記信頼された管理機関と共有される秘密鍵（ｓｅｃｒｅｔ　ｋｅｙ）でもよい。ドメイン管理機関も同様な方法で設定され、証明される。ユーザが１台のユーザ機器をあるドメインに登録したい場合、当該ユーザ機器とドメイン管理機関は互いの認証のために一つのプロトコルを用いる。この認証は、ユーザ機器とドメイン管理機関とに前もって組み込まれた公開鍵／共有鍵証明書に基づく標準的な方法を用いて実施される。認証が済めば、ドメイン管理機関は新規ドメインのためのドメイン証明書を作成してユーザ機器に送る。このドメインに新しいコンテンツが購入されるときは、コンテンツプロバイダにこの証明書が送られる。ユーザ機器のドメイン証明書を入手したコンテンツプロバイダは、証明書中の情報を用いてコンテンツを当該ドメインに割り当てることができる。なお、上記の各手続は公開鍵暗号法または共通鍵暗号法のどちらを用いても実施することができる。鍵の配布は、公開鍵暗号法を用いる方が共通鍵暗号法と比較して簡単である。

【００３０】

要求されたコンテンツは、最初はコンテンツプロバイダまたはデジタル著作権管理システム内の当該コンテンツにアクセス可能な他の構成要素から、コンテンツパッケージの一部として提供される。図７を参照すると、コンテンツパッケージ７００の全体構成の一例が示されている。コンテンツパッケージ７００は、ヘッダ（ＣＰＨ）７１０、権利文書（Ｒｄｏｃ）７２０、電子権利テーブルまたは符号化権利テーブル（ＥＲＴ）７３０、ハッシュテーブル７４０および暗号化コンテンツ７５０の５個のオブジェクトの連結によりなる。ヘッダ（ＣＰＨ）７１０は、主にコンテンツパッケージ７００の各オブジェクトの存在およびそのサイズを示すために使用される。コンテンツの使用規則は権利文書７２０に明記されている。これらの規則は一般には標準的フォーマットで記載される。権利文書は更に、前記証明書、公開鍵、およびユーザ機器が前記規則やコンテンツパッケージ内の他のオブジェクトの完全性を確認するために必要ないくつかのハッシュ値を含む。

【００３１】

コンテンツパッケージには、権利文書を更に効率的に表現したテーブルとしての符号化権利テーブル（ＥＲＴ）７３０も含まれる。この符号化権利テーブルの手法は、ＸｒＭＬ等の形式言語の手法とは異なるデータの二進表現を具現化し、また低パワーで制約の多いユーザ機器にとって特に魅力的である小サイズ・高速性を有する点で重要である。なお、制約された機器とは、処理能力やタスクローディングの制約、電源／バッテリーの不安要素、大容量記憶装置の制限、当該機器と他のインフラ要素との間の帯域上の制約等に基づいて画面サイズ、ＲＡＭ容量、ＲＯＭ容量等の物理的特徴が決められてしまうような通信機器を指す。

【００３２】

符号化権利テーブル７３０は、他の権利文書のデジタル使用権を本発明の符号化権利テー

ブルフォーマットに書き替えることが可能なように設計されている。つまり、符号化権利テーブルを使用するシステムが（それなしでは制約された機器への負荷が過大となるような）他のデジタル著作権管理システムと共存できるように設計されている。一つのデジタル著作権管理言語から符号化権利テーブルの表現への書き替えは、トランスコーダ（ｔｒａｎｓｃｏｄｅｒ）を用いて行うことができる。トランスコーダは元言語のデータを構文解析して符号化権利テーブルのフォーマットへと再コード化したり逆の作業を行ったりするものである。コンテンツプロバイダやデジタルコンテンツの所有者は、必要に応じて翻訳（変換）ソフトウェアを用いながら、自由に好みのデジタル著作権管理システムを選択することができる。

【００３３】

符号化権利テーブルには、予め指定された符号語またはトークンを用いて記述されたいくつかの部分（ＥＲＴ＿ＶＥＲＳＩＯＮ、ＴＯＫＥＮ＿ＯＢＪＥＣＴ＿ＩＮＦＯ、ＴＯＫＥＮ＿ＷＯＲＫ＿ＨＡＳＨ、ＴＯＫＥＮ＿ＫＥＹ＿ＩＤ、ＴＯＫＥＮ＿ｘｘｘ＿ＲＩＧＨＴ、ＴＯＫＥＮ＿ＥＲＴ＿ＳＩＧ等）がある。このＥＲＴ＿ＶＥＲＳＩＯＮ部は当該符号化権利テーブルのバージョン番号を与えるものである。符号化権利テーブルのフォーマットの以後のアップデートでは、その新バージョンが新しくなったソフトウェアから認識される必要があり、また後方互換性を保つため以前のバージョンも認識されることが必要とされる。ＴＯＫＥＮ＿ＯＢＪＥＣＴ＿ＩＮＦＯ部は、当該符号化権利テーブルに関連付けられたデジタル物品に関する情報、例えばそのデジタル物品のコピーを購入したりさらなる情報を得たりするためのＵＲＬ等を保持する。ＴＯＫＥＮ＿ＷＯＲＫ＿ＨＡＳＨ部は、当該符号化権利テーブルに関連付けられたデジタル物品の暗号ハッシュを含み、どのハッシュアルゴリズムを用いるべきかを示す。ＴＯＫＥＮ＿ＫＥＹ＿ＩＤ部は、当該デジタル物品へのアクセスに必要な鍵を指定する。この鍵の一例としては、公開鍵暗号アルゴリズムを用いて受取人に割り当てられるコンテンツ暗号化鍵（ＣＥＫ：Ｃｏｎｔｅｎｔ　Ｅｎｃｒｙｐｔｉｏｎ　Ｋｅｙ）が可能である。ＴＯＫＥＮ＿ｘｘｘ＿ＲＩＧＨＴ部（ｘｘｘは任意文字）は当該デジタル物品の使用規則を含む。一例として、ＴＯＫＥＮ＿ＰＬＡＹ＿ＲＩＧＨＴ部を設け、ＴＯＫＥＮ＿ＫＥＹ＿ＩＤ部に書かれた特定の鍵に当該デジタル物品の「ＰＬＡＹ」権が与えられていることを明記する等のことが可能である。この符号化権利テーブル仕様書に盛り込むことが可能な他の権利としては、ストリーミング、貸与、コピー、転送、インストールなどがある。各権利の記載には、その権利が当てはまる当該デジタル物品の部分を特定する情報も含まれる。最後にＴＯＫＥＮ＿ＥＲＴ＿ＳＩＧ部は、符号化権利テーブルデータのハッシュに署名するために用いられた署名アルゴリズムを特定する情報、署名者の公開鍵または共通鍵、および署名データそのものを含む。

【００３４】

コンテンツプロバイダ２１０は、前記規則の実施の複雑さをより軽減するために上記符号化権利テーブル７３０をコンテンツパッケージ７００に添付する。コンテンツパッケージのサイズがわずかに増し、コンテンツプロバイダによる若干の前処理作業が必要となるものの、符号化権利テーブルを用いることで、ユーザ機器上のソフトウェアをより簡素化することが可能となる。

【００３５】

コンテンツの完全性やコンテンツと権利文書との結合は、ハッシュを用いて維持することができる。ハッシュはコンテンツパッケージの完全性の確認方法を可能とする。コンテンツパッケージの最後の部分は、暗号化コンテンツ７５０（暗号化されたコンテンツ）そのものである。コンテンツは、海賊行為を防止するために暗号化状態に保たれる。コンテンツ用の暗号解読鍵は権利文書に組み込まれ、当該コンテンツの所有者または購入者のみが利用できる。

【００３６】

図７に点線で示したように、コンテンツパッケージ７００内の複数のオブジェクトを２個のファイルとして提供することも選択可能である。図７の例では、コンテンツプロバイダヘッダ（ＣＰＨ）、ＲＤｏｃおよび符号化権利テーブルを含むライセンスファイル７６０

と、コンテンツのハッシュ、暗号化コンテンツおよび図示しないコンテンツパッケージヘッダ７１０の複製を含む暗号化コンテンツファイル７７０とに分けられている。

【００３７】

以下において、本発明によるユーザ機器の構成および好適な動作について述べる。図８を参照すると、ドメインベースのデジタル著作権管理環境において動作可能なユーザ機器２０２（携帯電話機等）のブロック図８００が示されている。この通信機器（ユーザ機器）は、ＣＰＵ素子８０２とデジタル著作権管理（ＤＲＭ）モジュール８０４を有しており、デジタル著作権管理（ＤＲＭ）モジュール８０４はドメインベースの環境において送信部８０６および受信部８０８の動作を制御可能なソフトウェアまたはファームウェアを含む。このユーザ機器は、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）８１０、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）８１２、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）８１４等のメモリ素子のほか、随意的に取り外し可能なコンテンツ記憶装置８１６を備える。電源／直流制御ブロック８２４および充電式バッテリー８２６によりユーザ機器２０２に電力が供給される。以下で明らかになるように、前記デジタル著作権管理モジュールのソフトウェアまたはファームウェアは、ドメイン管理機関と協働して当該ユーザ機器を１つ以上のドメインに加入または脱退させ、従って前記ドメインのメンバーシップに基づいて選択的にコンテンツを受信し、その暗号解読を行う。ユーザ機器は更に、当該ユーザ機器のユーザとのインターフェースとしてのキーボード８１８、ディスプレー８２０、ヘッドホン８２２等の周辺部品を有していてよい。

【００３８】

図９のブロック図９００に、代表的なユーザ機器の構成を示す。図には、ユーザ機器２０２においてコンテンツの安全なアクセス、管理、表現を担当する種々のメモリやソフトウェア部品が示されている。この代表例において、コアとなるデジタル著作権管理ソフトウェア９０２（図ではデジタル著作権管理モジュールとして点線に囲まれている）は、コンテンツパッケージ管理部９０４、通信管理部９０６、コンテンツ復号部９０８、およびコンテンツプレーヤー９１０により構成されている。なお、このデジタル著作権管理ソフトウェア９０２のこれらの部品の機能性を本発明の精神と範囲から逸脱することなく他の構成を用いて実現してもよいことはもちろん理解されるはずである。このデジタル著作権管理モジュールのコアソフトウェアは、暗号解読されたコンテンツを取り扱い、安全に保つ責任を負う。このコアに加え、ファイルや鍵の管理、ネットワーキング、種々の暗号機能等の作業を行うための種々の階層の支援ソフトウェアが必要となる。また、ユーザがコンテンツを購入しアクセスするために立ち上げることができるアプリケーションが２つある。コンテンツ管理アプリケーション９１２とウェブブラウザアプリケーション９１４である。ここに記載の各アプリケーションソフトウェアは、ウイルスを含まず、安全に保護されるデータや鍵を危険にさらさないことが確認されているという意味で、信頼されていることが前提となっている。信頼された構成要素、例えば機器製造業者は、ユーザ機器のソフトウェアおよびアプリケーションがこれらの規則に準拠していることを確認する義務を有する。

【００３９】

ユーザ機器が受信した暗号化コンテンツは、図に示すように、ユーザ機器の不揮発性メモリ９１８内に格納されるコンテンツパッケージ９１６中に保存することができる。この不揮発性メモリはオープンアクセスメモリであり、当該メモリへのアクセスの制限によってではなくコンテンツパッケージ中のコンテンツの暗号化によってそのセキュリティーが維持される。ユーザ機器におけるオープンアクセスメモリは内蔵でも外付けでもよい。一方、特定のユーザ機器やドメインに結合された公開データ、例えば公開鍵証明書は、内部メモリ９２０に格納されるのが望ましい。これよりサイズが大型になりやすいコンテンツパッケージは、外付けの取り外し可能なフラッシュメモリカード、例えばＭＭＣ（ＭｕｌｔｉＭｅｄｉａ Ｃａｒｄ）に格納することができる。

【００４０】

上記オープンアクセスメモリ９１８および９２０は、ファイルシステム管理部９２２を用いて管理される。このファイル管理部は、下位の各入出力ルーチンを含むファイル操作を担当する。より上位のアプリケーションソフトウェアは、このファイル管理部を通じてオープンアクセスメモリ内のファイルの生成、変更、読み込みおよび整理を行う。例えば、当該ユーザ機器のウェブブラウザアプリケーション９１４がコンテンツパッケージをオンラインコンテンツプロバイダから購入するのに使用されることがあり、ユーザは新しく購入したコンテンツパッケージを取り外し可能なメモリカードにコピーしたいと思う場合がある。このような新しいコンテンツパッケージには、ある支援アプリケーションに関連付けられた特定のファイル拡張子（例えば「．ｃｐｋ」）が付けられており、上記ブラウザによるコンテンツパッケージのダウンロードが終了すると、そのコンテンツパッケージのインストールのために上記支援アプリケーションが立ち上げられる。そして、この支援アプリケーション（コンテンツインストーラ９２４）は、前記ファイルシステム管理部に指示して新しく受信されたコンテンツの格納を行う。

【００４１】

上記のウェブブラウザ９１４は、ユーザがドメインに加入／脱退したい場合にも使用できる。この好適な実施形態においてドメインに加入する場合には、ユーザは該ドメインの秘密鍵（ｐｒｉｖａｔｅ　ｋｅｙ）と公開鍵証明書を入手するためにドメイン管理機関のウェブサイトを訪れる。ブラウザはこれらのデータを安全にダウンロードし、鍵／証明書インストーラプログラム９２６がこの新しい鍵と証明書を自動的にインストールする。このインストーラプログラム９２６は入力された鍵を暗号解読し、ユーザ機器の保護メモリ９３０を管理するソフトウェアモジュール９２８にこれを渡さなければならない。

【００４２】

ユーザ機器の保護メモリ（ｓｅｃｕｒｅ　ｍｅｍｏｒｙ）としては２種類のものが用いられている。第１のタイプは、不正改竄発見機能付き（ｔａｍｐｅｒ－ｅｖｉｄｅｎｔ）メモリ９３２である。この好適な実施形態において、不正改竄発見機能付きメモリは、機器の暗号化された秘密鍵（ｐｒｉｖａｔｅ　ｋｅｙ）、例えば一意のユニット鍵（ＫｕＰｒｉ）や共有されたドメイン鍵（ＫｄＰｒｉ）などの格納に用いられる。更に例えばペイ・パー・プレーやワン・タイム・プレーなどのデジタル著作権管理業務の追跡データ、および当該ユーザ機器用のソフトウェアもこのメモリに格納される。安全な暗号ハッシュ値および署名を用いてメモリの完全性が確認されるため、このメモリは不正改竄発見機能を持つことになる。

【００４３】

上記不正改竄発見機能付きメモリのためのハッシュ値は、保護メモリの第２のタイプである不正改竄防止機能付き（ｔａｍｐｅｒ－ｒｅｓｉｓｔａｎｔ）メモリ９３４に格納される。このタイプのメモリは、ハッカーによるメモリ内容の読み出しや変更の試みに耐えることができる。この好適な実施形態において、前記一意のユニット鍵（ＫｕＰｒｉ）や共有されたドメイン鍵（ＫｄＰｒｉ）の暗号化に用いられる機密度の高い鍵が、この不正改竄防止機能付きメモリに格納される。また、ユーザ機器のソフトウェアの安全な動作を保証するためのブートコードやルート鍵もこのメモリ内に保持される。上記ブートコードは、ユーザ機器のオペレーティングシステムの起動や、ユーザ機器上のソフトウェアの完全性の確認において極めて重要なコードである。

【００４４】

この保護メモリ９３２および９３４は、保護メモリ管理部９３０を通じてアクセスされる。この管理部は、不正改竄発見機能付きメモリ９３２へのデータの入出力や不正改竄防止機能付きメモリ９３４に格納された対応するハッシュ値の更新を担当する。保護メモリ管理部９３０はまた、不正改竄発見機能付きメモリ９３２への不正改竄の有無のチェックも行う。鍵／証明書／デジタル著作権管理アカウント管理部９２８は、新しい鍵やデジタル著作権管理業務によって保護メモリの更新の必要が生じた場合はいつでも保護メモリ管理部９３０へのインターフェースを行う。

【００４５】

デジタル著作権管理支援ソフトウェアの最後の部分は、各ネットワークレイヤ９３６である。特に、ＳＳＬ、ＴＬＳ、ＷＴＬＳ等の安全なネットワークレイヤ９３８がデジタル著作権管理アプリケーションによって利用される。これらの各セキュリティーレイヤにより、ネットワーク９４０内のユーザ機器とサーバ（ドメイン管理機関、コンテンツプロバイダ、他のユーザ機器等）間に安全な通信チャンネルを確立するための標準的方法がもたらされる。これらのネットワークレイヤには、当該デジタル著作権管理モジュールのコアソフトウェアの一部である前記デジタル著作権管理通信管理部以外にも、前記ブラウザアプリケーションがアクセスする。

【００４６】

ユーザ機器のデジタル著作権管理コアソフトウェア（「通信装置のデジタル著作権管理モジュール」と呼ぶ）は、暗号解読されたコンテンツを安全に取り扱うとともに、ユーザがコンテンツの表現や操作のために実行するコンテンツ管理アプリケーションによって利用される。音楽の場合には、このコンテンツ管理アプリケーションは、曲の演奏やプレイリストの生成に使用されるアプリケーションであり、そのユーザインターフェースは、曲のタイトル、演奏時間、アーティスト名などの曲情報を表示する。このアプリケーションはまた、ピアツーピア接続の管理やドメイン選択の制御のためのユーザインターフェースを与える。また、どのコンテンツパッケージが演奏可能かを常に把握できるように、コンテンツ管理アプリケーションは一般にファイルシステム管理部への直接接続を有している。

【００４７】

ユーザがあるコンテンツの表現を決めた場合、コンテンツ管理アプリケーションによってデジタル著作権管理コアソフトウェアが呼び出される。この基本的なコンテンツプレーヤーはコンテンツを表現して出力装置に出力するが、その表現の前にコンテンツの復号化が必要であり、また、その復号化の前に暗号解読が必要である。コンテンツパッケージ管理部は、コンテンツパッケージを処理し、暗号解読することが可能なソフトウェアモジュールである。

【００４８】

また、コンテンツ復号化ソフトウェア（コンテンツ復号部）は、コンテンツパッケージ管理部にコンテンツパッケージの「開封」を指示する。該コンテンツパッケージは、その権利文書、ハッシュおよび符号化権利テーブルが確認されることによって、「開封」される。規則がパッケージの開封およびアクセスを許可していることが確認されると、コンテンツパッケージ管理部は当該暗号化されたコンテンツの読み込みや暗号解読を開始する。暗号解読されたコンテンツはバッファーを介してコンテンツ復号部へ送られ、コンテンツ復号部は該コンテンツをデータ復元し、これを表現のために基本コンテンツプレーヤーに渡す。ここでコンテンツパッケージ管理部が規則違反を発見すれば、エラーコードが返される。コンテンツパッケージ管理部はまた、あるコンテンツの表現のために更新が必要な場合はいつでも、鍵／証明書／デジタル著作権管理アカウント管理部に連絡してデジタル著作権管理アカウントデータを更新する。

【００４９】

このデジタル著作権管理コアルーチンにおける通信管理部は、他の機器への通信リンクの設定を行う。これらのリンクは、ストリーミング、コピー、貸与、他の信頼された機器へのコンテンツの転送等に用いられる。安全なチャンネルの確立のために、通信管理部は可能な限りネットワークソフトウェアのセキュリティー部品を利用する。

【００５０】

次に、図１０を参照すると、ドメインベースのデジタル著作権管理システムおよび方法におけるドメイン管理機関２０４の動作、およびユーザ通信機器のドメインへの登録および削除を安全に行うためにドメイン管理機関により用いられる様々な要素を示すブロック図１０００が示されている。破線で囲まれたデジタル著作権管理コアソフトウェアおよび／またはファームウェア１００２は、この好適な実施形態におけるウェブサーバアプリケーションであり、通信管理部１００４、機器登録管理部１００６、ドメイン鍵パッケージング部１００８、および不正／取消検出部１０１０により構成されている。また、このドメ

イン管理機関２０４におけるデジタル著作権管理コア支援ソフトウェア１００２は、前記ウェブサーバアプリケーションにより起動される各々の共通ゲートウェイインタフェース（ＣＧＩ）プログラムによってアクセスされる。これらの共通ゲートウェイインタフェース（ＣＧＩ）プログラムは上記デジタル著作権管理コアソフトウェアの一部をなすものである。また前述のユーザ機器の場合と同様に、このコアに加えて、メモリ管理、ネットワーキング、種々の暗号機能等の作業を行うための種々の階層の支援ソフトウェアが必要となる。

【００５１】

証明書管理機関と同様に、当該ドメイン管理機関は物理的攻撃から守られた環境において動作する信頼されたサーバであることが前提となっている。このドメイン管理機関における支援ソフトウェアは、例えば、秘密ドメイン鍵、すべての登録された機器および未登録の機器のリスト、ドメイン登録活動の履歴、機器の登録取消のリスト、および信頼されたデジタル著作権管理ソフトウェアなどからなる秘密データのセキュリティーの維持を担当する。これらのデータは、不正改竄発見機能付きメモリ１０２０に格納するのが好ましく、また、その一部を暗号化して格納するのが好ましい。

【００５２】

不正改竄発見機能付きメモリ１０２０内の不正改竄の検出には、不正改竄防止機能付きメモリ１０２２が必要となる。以前にユーザ機器の場合で述べたように、不正改竄発見機能付きメモリ１０２０にデータを入出力し、不正改竄防止機能付きメモリ１０２２内の関連したハッシュ値を適切に更新するために、保護メモリ管理部１０２４が用いられる。

【００５３】

この好適な実施形態において、ドメインデータ、鍵および証明書の不正改竄発見機能付きデータベースは、ドメイン／デジタル著作権管理データ管理部１０２６により管理される。このデータベース管理部１０２６に対しては、特定のユーザ機器に属するドメイン鍵や、特定のドメインに属するユーザ機器に関しての問い合わせを行うことができる。また、各々のドメイン管理機関は、当該ドメイン管理機関をユーザ機器に対して証明するためのドメイン管理機関証明書１０２８をオープンアクセスメモリ１０２９内に保持する。安全な通信チャンネルが確立される過程において、このドメイン管理機関証明書（ＤＡＣｅｒｔ）が証明書管理機関によって署名されユーザ機器との間で交換される。前記オープンアクセスメモリ１０２９は、ファイルシステム管理部１０３０を用いて管理される。このファイル管理部は、下位の各入出力ルーチンを含むファイル操作を担当する。より上位のアプリケーションソフトウェアは、このファイル管理部を通じてオープンアクセスメモリ内のファイルの生成、変更、読み込みおよび整理を行う。

【００５４】

このドメイン管理機関のデジタル著作権管理コアソフトウェアは、当該ドメイン管理機関とユーザ機器との間の対話および当該ドメイン管理機関とコンテンツプロバイダとの間の通信を処理する。当該ドメイン管理機関のデジタル著作権管理ソフトウェアの主な構成要素は、前記ウェブサーバアプリケーションである。このウェブサーバは、ウェブページ、例えばＷＡＰ仕様のユーザ機器のためのＷＭＬ形式のウェブページをユーザ機器に対して提供する。これらのウェブページは、ユーザがドメインに対する機器の加入／脱退を容易に行えるようにするためのユーザインターフェースの一部をなす。

【００５５】

機器をドメインに加入させるためのウェブページは、まず、ユーザが既存のドメインに機器を加入させたいのか、新しくドメインを生成したいのかを確認する。新規ドメインの生成の場合は、ユーザはドメイン名とパスワードの選択を求められる。ある好適な実施形態においては、ドメイン管理機関はその後ユーザ機器との間に安全な認証された接続を例えばＷＡＰクラス３プロトコルまたは同等のプロトコルを用いて確立する。この安全なチャンネルの確立中にドメイン管理機関は、ユーザ機器の、工場で設定された一意のユニット公開鍵を検出する。ドメイン管理機関の機器登録プログラムは、新規ドメインを当該ドメイン管理機関のデジタル著作権管理データベース内に設けるために、この公開鍵、そして

ドメイン名およびパスワードを用いる。最後に当該ドメイン管理機関は、この新規ドメインのための新規の秘密鍵と公開鍵の対を生成し、この秘密鍵とその使用のための指示書を、ユーザ機器によりダウンロードされるファイル内に格納する。ユーザ機器の鍵インストーラアプリケーション１０３２は、この鍵ファイルを構文解析して前記指示書と新規ドメイン鍵を入手する。前記指示書は、ユーザ機器に当該鍵をメモリ内にインストールするよう指示し、これによりユーザ機器が当該ドメインに登録される。

【００５６】

一方、ユーザが機器を既存のドメインに加入させたい場合には、手順は極めて簡単なものとなる。ユーザは、既存ドメインの名称とパスワードを尋ねられ、ドメイン管理機関はそのドメインを調べ、パスワードを確認し、前記ドメイン内の機器数がその上限に達していないかを確認する。上限に達していなければ、ドメイン管理機関はユーザ機器をそのドメインに加入させ、そのドメインの秘密鍵を引き出してパッケージし、これを安全な認証されたチャンネルを介してユーザ機器に与える。

【００５７】

ユーザが機器をドメインから脱退させたい場合、ドメイン管理機関はまず、ユーザ機器の公開鍵を調べて認証するために安全なチャンネルを確立する。次にドメイン管理機関は、この公開鍵を自身のデータベースで検索し、そのユーザ機器がどの（１または複数の）ドメインの会員であるかを調べる。次にユーザ機器のユーザは、当該ユーザ機器のどのドメインの会員権を抹消したいかを選択するよう求められる。ドメイン管理機関はその情報を処理して当該ユーザ機器によってダウンロードされることになる鍵消去パッケージを生成する。ユーザ機器の鍵インストーラプログラム１０３２は、このパッケージを構文解析し、適切な鍵を消去した後、ドメイン管理機関に確認メッセージを送信する。これにより、ドメイン管理機関は当該ユーザ機器が既にそのドメインの会員ではないことを確認することができる。

【００５８】

ドメイン管理機関はまた、各ユーザ機器が行うドメインへの登録／登録抹消の試みに関する履歴を記録している。この履歴は不正／取消検出部１０１０によって監視され、疑わしい行動が検出された場合にはドメイン管理機関のシステムオペレーターに警告メッセージが発せられる。システムオペレーターは、その疑わしい行動を取っているユーザ機器の公開鍵を取り消すべきか否かを決定するために更なる調査を開始することができる。また、必要に応じてドメイン管理機関は取消を受けたユーザ機器のリストを取り、リストに掲載されたユーザ機器へのサービスを許否することもできる。

【００５９】

ドメイン管理機関はまた、コンテンツプロバイダと通信する機能を有している。あるユーザ機器にコンテンツを売る場合、コンテンツプロバイダは当該ユーザ機器が会員になっているドメインのリストをドメイン管理機関に要求し、この要求はドメイン管理機関の通信管理部によって処理される。コンテンツプロバイダが得るこの情報により、これらのドメインの一つのためにコンテンツを購入する際の便利な方法を当該ユーザ機器のユーザに提供することが可能となり、当該ユーザ機器との取引が容易なものとなる。ドメイン管理機関とコンテンツプロバイダが通信を望まない場合には、当該ユーザ機器のユーザが上記ドメインに関する情報を提供することとなる。

【００６０】

次に、図１１を参照すると、ドメインベースのデジタル著作権管理環境において要求されたコンテンツの供給に適したコンテンツプロバイダ２１０の構成を示すブロック図１１００が示されている。このコンテンツプロバイダにおいて、破線で囲まれたデジタル著作権管理コアソフトウェアおよび／またはファームウェア１１０２は、通信管理部１１０４、コンテンツパッケージング部１１０６、および取消検出部１１０８の機能を有している。本発明の一つの好適な実施形態では、この機能はウェブサーバアプリケーションによって与えられる。このコンテンツプロバイダの支援ソフトウェアは、メモリ管理、ネットワーキング、種々の暗号機能等の作業を行う。

【００６１】
前述のユーザ機器やドメイン管理機関の場合と同様に、コンテンツプロバイダの秘密鍵、取消リスト、およびすべての信頼されたソフトウェアを格納するために、不正改竄発見機能付きメモリ１１１０が用いられる。コンテンツパッケージ１１１２はオープンアクセスメモリ１１１４内に保持され、これらのパッケージは当該コンテンツプロバイダの公開鍵に割り当てられる。従ってコンテンツは、コンテンツプロバイダの秘密鍵によってのみ暗号解読可能な鍵を用いて暗号化される。そして、あるユーザ機器がコンテンツパッケージを購入する場合には、当該コンテンツプロバイダのデジタル著作権管理コアソフトウェアがこのコンテンツパッケージを当該ユーザ機器の公開鍵に割り当て直す。

【００６２】
このコンテンツプロバイダのデジタル著作権管理コアソフトウェア１１０２は、当該コンテンツプロバイダ２１０とユーザ機器２０２との間の対話および当該コンテンツプロバイダ２１０とドメイン管理機関２０４との間の通信を処理する。当該コンテンツプロバイダのデジタル著作権管理ソフトウェアの主な構成要素は、一つの好適な実施形態によるウェブサーバアプリケーションである。このアプリケーションは、ウェブページ、例えば、ＷＡＰ仕様のユーザ機器のためのＷＭＬ形式のウェブページをユーザ機器に対して提供する。これらのウェブページは、ユーザがドメイン機器のためにコンテンツを購入する際に使い勝手のよいインターフェースを提供する。

【００６３】
ブロック図におけるその他の部品（オープンアクセスメモリ１１１６、保護メモリ管理部１１１８、鍵／証明書管理部１１２０、不正改竄防止機能付きメモリ１１２２、ネットワーク１１２４、各ネットワークレイヤ１１２６、鍵／証明書インストーラ１１２８等）の機能は、図９および図１０を参照して説明した類似名称の部品の機能と同様である。

【００６４】
要求されたコンテンツをユーザに提供するために安全な認証されたチャンネルを確立する場合、一つの好適な実施形態によれば、コンテンツプロバイダがユーザ機器の秘密鍵を入手する。コンテンツプロバイダは次にドメイン管理機関と連絡を取って当該ユーザ機器が属している１つ以上のドメインを調べることができる。そして、コンテンツプロバイダは任意に作成したウェブページ上で、ユーザ機器のユーザに新しいコンテンツをどのドメインに割り当てるかを決定させることができる。その後コンテンツプロバイダは、当該コンテンツをこの希望されたドメインに割り当て直す。なお、ユーザ機器のユーザに、音楽（コンテンツ）を購入して割り当てたいドメインのドメイン名（またはＵＲＬ）を手入力させることも可能である。そして、コンテンツプロバイダは再びドメイン管理機関に連絡を取り当該ドメインの公開鍵証明書を入手し、これによりコンテンツパッケージは当該ドメインに割り当てられる。

【００６５】
この新しく割り当て直されたパッケージは前記ユーザ機器に転送され、その後ユーザ機器にインストールされる。また、ユーザが当該コンテンツをオンラインコンテンツアカウントにも送りたくなる可能性もあるが、このような場合、コンテンツプロバイダは当該コンテンツパッケージに指示書を添えて適切なコンテンツバンクへ転送することもできる。

【００６６】
また、コンテンツプロバイダは、所定のウェブページが参照された際に呼び出される様々な共通ゲートウェイインタフェース（ＣＧＩ）プログラムを有している。その一例が当該コンテンツプロバイダとドメイン管理機関との間の対話を処理する前記通信管理部１１０４である。コンテンツパッケージは、コンテンツパッケージング部１１０６と呼ばれる別のＣＧＩプログラムを用いてユーザ機器に割り当て直される。そして最後に、コンテンツ購入中のユーザ機器の公開鍵が取り消されたものでないことの確認が、もう一つのＣＧＩプログラムである取消検出ソフトウェア１１０８を用いて行われる。

【００６７】
以上に説明したように、本発明のドメインベースの手法によれば、消費者をデジタルコン

テンツにアクセスさせるための利便性の高い方法として、従来のコピーベースの手法における煩わしいチェックイン／チェックアウト方針を用いずにデジタルコンテンツの海賊行為を防止可能な方法を得ることができる。コンテンツへのアクセスは１つ以上のドメインにおける登録した機器に限られるが、登録したドメイン機器からは、いつでもどこでもコンテンツへのアクセスが可能となる。ドメイン外の信頼された機器は、ドメイン内のコンテンツに対して自動的にアクセス可能とはならないが、適切なコンテンツ用プロトコルに対応していればコンテンツを入手することができる。登録された機器のみにコンテンツへのアクセスが許可されるため、チェックイン／チェックアウト方針が不要となり、手続が大幅に簡素化し、ユーザの体験は大きく広がることになる。エンドユーザがセキュリティーに遭遇するのは新しい機器を１つ以上のドメインに加入させるときのみとなるが、各コンテンツは強力な暗号化／セキュリティープロトコルに基づく暗号技術を用いて保護されるため、セキュリティーは強固なまま保たれる。

【００６８】

以上、本発明を具体的な各実施の形態を用いて説明してきたが、上記内容を考察すれば多くの代替例、変更、並べ替え、変形例等が通常レベルの当業者に容易に想到可能であることは明らかである。従って本発明は、そのような代替例、変更、変形例等のすべてが添付された請求項の範囲内のものとして包含されるよう意図されている。例えば、本発明は、ポケベル、携帯電話機、ＰＣＳ機器、およびブルートゥース機器（限定された通信範囲を特徴とする）などの携帯型無線機器のみならず、必ずしも携帯型や無線式でない、自動車用娯楽システム、デジタルコンテンツ対応のセットトップボックス、家庭用コンピュータなどの機器にも応用可能である。

【図面の簡単な説明】

【００６９】

【図１】従来のコピーベースのデジタル著作権管理システムを示すブロック図。

【図２】本発明の一実施形態によるドメインベースのデジタル著作権管理システムの各構成要素を示す模式図。

【図３】本発明による重複したドメインを示す模式図。

【図４】本発明によるドメインベースのデジタル著作権管理システムを示すブロック図。

【図５】本発明による１つ以上のユーザ通信機器を有したドメインを示す概念図。

【図６】本発明によるコンテンツのドメインへの結合の仕方を示す模式図。

【図７】本発明によるコンテンツパッケージをの一例を示す模式図。

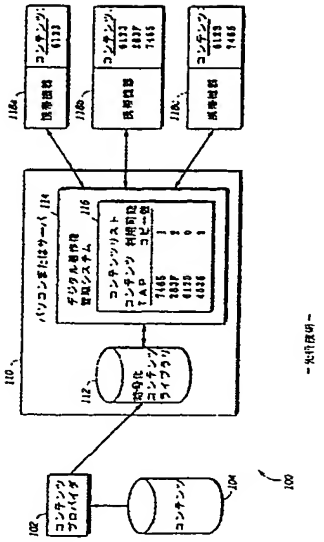
【図８】本発明によるユーザ通信機器のブロック図。

【図９】本発明によるユーザ機器の構成を示すブロック図。

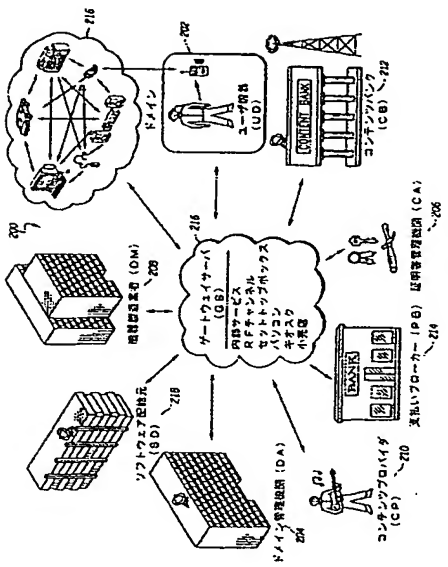
【図１０】本発明によるドメイン管理機関の構成を示すブロック図。

【図１１】本発明によるコンテンツプロバイダの構成を示すブロック図。

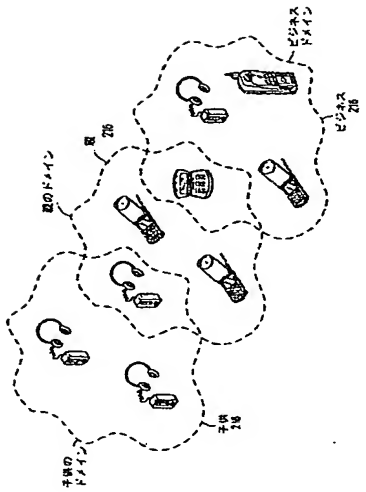
【図１】



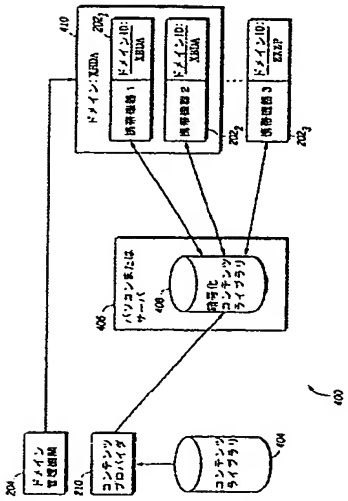
【図２】



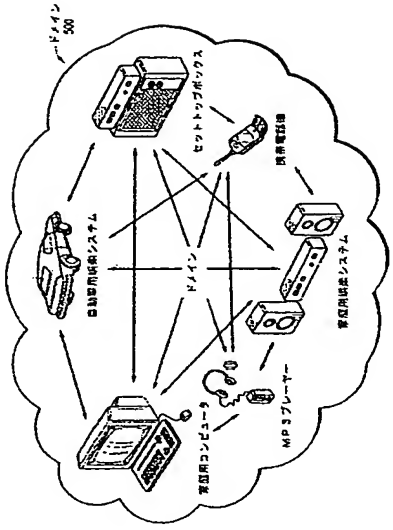
【図３】



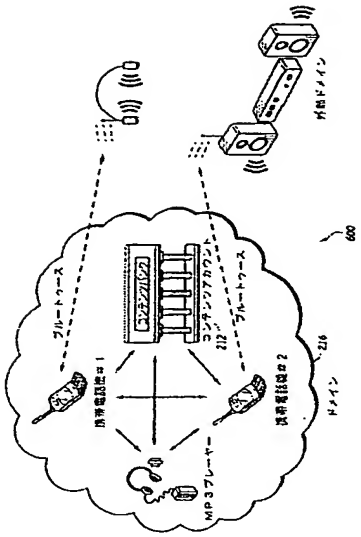
【図４】



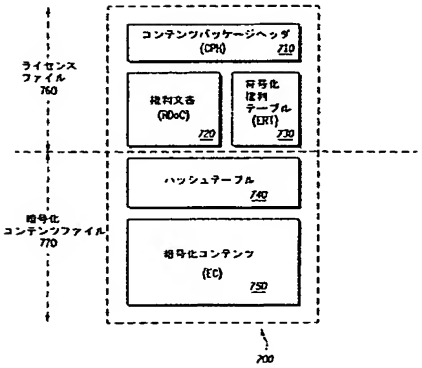
【図５】



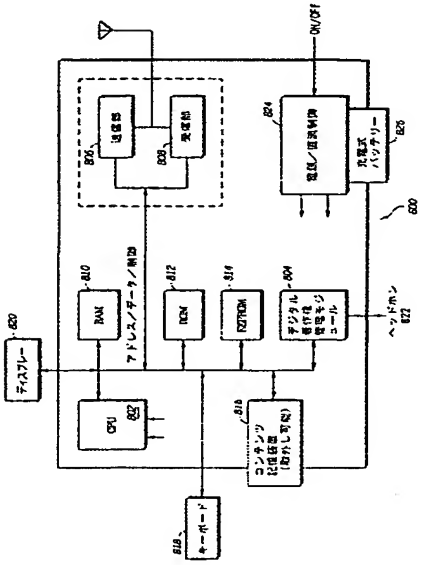
【図６】



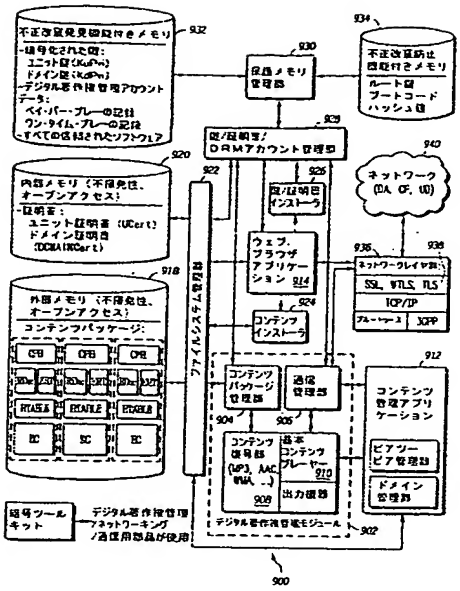
【図７】



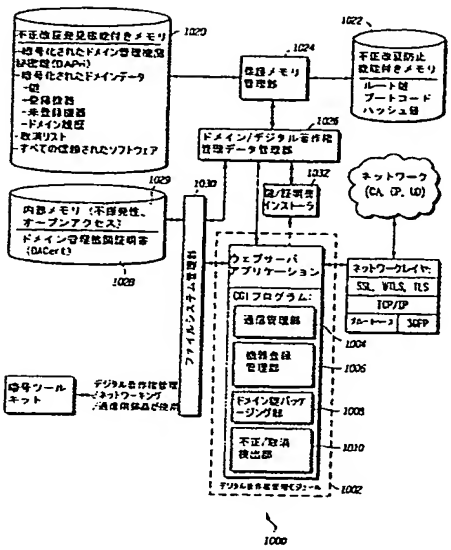
【図８】



【図９】



【図１０】



【図１１】